รปภ. คอมพิวเตอร์

ขั้นตอนง่าย ๆ ในการปกป้องข้อมูล หรือระบบคอมพิวเตอร์ ที่กระทำได้ด้วยตัวเอง

ระบบคอมพิวเตอร์ได้เข้ามามีบทบาทมากในองค์กรธุรกิจต่าง ๆ ในปัจจุบัน ไม่เว้นแม้กระทั่งในโรงงาน โรงเรียน และในบ้าน ถือได้ว่าเป็นเครื่องมือเครื่องใช้ประจำครัวเรือนไปแล้ว ซึ่งตอบสนองความต้องการใช้งานได้สำหรับทุกคนในครอบครัว ด้วยประสิทธิภาพที่สูงขึ้น ทำให้การใช้งานและการทำงานมีประสิทธิภาพมากขึ้น

แต่สิ่งที่กำลังคืบคลานเข้ามาทำให้ผู้ใช้งานหรือเจ้าของกิจการที่ใช้คอมพิวเตอร์ต้องปวดหัว เป็นเรื่องของระบบการรักษาความปลอดภัย ไม่ใช่ รปภ. นะครับ เป็นระบบรักษาความปลอดภัยในคอมพิวเตอร์

อย่างแรกที่คุ้นเคยกันเป็นอย่างดีคงจะหนีไม่พ้นเรื่องของไวรัสคอมพิวเตอร์ ซึ่งเป็นสาเหตุใหญ่ที่ทำให้ข้อมูลสูญหาย ความสามารถของไวรัสได้ถูกพัฒนาขึ้นเรื่อย ๆ มีความสามารถในการซ่อนตัวและทำลายข้อมูลสำคัญให้ผู้ใช้คอมพิวเตอร์เจ็บใจเล่น

ความจริงในเรื่องของความปลอดภัยของข้อมูลหรือระบบคอมพิวเตอร์ ก็คงจะต้องกล่าวถึงเรื่องแฮกเกอร์หรือกลุ่มคนที่มีความสามารถสูงในด้านทักษะคอมพิวเตอร์ แต่นำความรู้นั้นมาใช้อย่างไม่ถูกต้องเท่าไร และเรื่องของไวรัสที่ทำลายข้อมูล สองประเด็นนี้คงเป็นเรื่องที่ต้องพูดถึงกันมาก

แต่ในทางปฏิบัติแล้วนั้นยังอาจมีประเด็นอื่นที่ต้องนำมาพิจารณาด้วย เช่น บุคลากรในองค์กรที่ชอบนำโปรแกรมไปใช้งานในทางผิด ๆ หรือการพาบุคคลภายนอกเข้าไปในที่ทำงาน ซึ่งอาจจะมีการจารกรรมข้อมูลหรือทำลายข้อมูลในระบบได้

ไวรัส

เป็นที่ทราบกันอย่างดีแล้วว่า ตัวการสำคัญที่ทำลายข้อมูลในระบบคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ ให้ทำงานผิดปกติ ทำให้เกิดผลกระทบกับการทำงาน อาจจะทำให้เกิดมูลค่าความเสียหายทางธุรกิจอย่างคาดไม่ถึง วิทยาการและความก้าวหน้าในการนำไวรัสมาใช้งานหรือทำลายได้อุบัติขึ้น ไวรัสที่เจอช่วงแรก ๆ จะติดกับโปรแกรมจำพวก .com และ .exe โดยจะทำงานก็ต่อเมื่อมีการเรียกใช้ไฟล์

ไวรัสมีความสามารถในการเข้าทำลายระบบจากแผ่นดิสค์ การถ่ายข้อมูลผ่านระบบเครือข่าย และฝังตัวอยู่ในหน่วยความจำ (memory resident) การทำงานของไวรัสอาจจะมีการทำงานในวันเวลาต่าง ๆ กัน เช่น ไวรัสวันศุกร์ที่ 13 เป็นต้น

ไวรัสติดต่อได้ทางไหนบ้าง แผ่นดิสค์ จากศูนย์บริการข้อมูล-ข่าวสาร (BBS-Bulletin Board System) การติดต่อหรือเชื่อมต่อระหว่างเครือข่ายคอมพิวเตอร์ และจากอินเทอร์เน็ต

จากที่เข้าไปฝังตัวและทำลายข้อมูลของไวรัส จะเริ่มปฏิบัติการทำลายหรือทำความเสียหายให้แก่ข้อมูลตามวันเวลาหรือเป้าหมายที่ได้กำหนดไว้ให้ทำลาย แล้วต้องทำอย่างไรสำหรับการป้องกันไวรัส คำแนะนำเบื้องต้นคือ ในด้านของการถ่ายข้อมูลและการจัดเก็บข้อมูล ไม่ควรนำไปรวมกับแผ่นระบบงาน (System disk) ไม่ควรเปลี่ยนแผ่นหรือถ่ายข้อมูลระหว่างระบบกับผู้ใช้คนอื่น เพราะอาจจะทำให้ติดไวรัสได้ง่ายขึ้น ควรมีการพิมพ์ขนาดของไฟล์หรือไดเรคทอรีเก็บไว้อ้างอิงอยู่เสมอ ในการเรียกใช้โปรแกรมาจากแหล่งอื่นที่ไม่มั่นใจว่าปลอดไวรัสหรือเปล่า และที่สำคัญควรมีการสแกนไวรัสจากทุกแผ่นดิสค์ที่จะนำมาใช้งานกับระบบคอมพิวเตอร์ เพื่อความมั่นใจอีกขั้นตอนหนึ่งต้องมีการสแกนไวรัสในระบบคอมพิวเตอร์ทุกสัปดาห์ หรือถ้าเป็นไปได้สแกนไวรัสทุกวันเลย ด้วยโปรแกรมตรวจจับไวรัสรุ่นใหม่ ๆ เช่น McAfec, PcCillin ฯลฯ

แฮกเกอร์ (Hacker)

เรื่องราวของแฮกเกอร์ได้เริ่มขึ้นตั้งแต่ปี ค.ศ. 1970 เป็นการลักลอบเข้าไปใช้โทรศัพท์ของ AT&T ด้วยการควบคุมความถี่ แต่ผู้เป็นตำนานและกล่าวขานกันมากที่สุดคือ Kevin Mitnick ที่ลักลอบเข้าสู่เครือข่ายคอมพิวเตอร์ต่าง ๆ ไม่ว่าเป็นการทำลายข้อมูลเครือข่ายคอมพิวเตอร์ของธนาคาร แอบเปลี่ยนรายงานสินเชื่อ แอบตัดสัญญาณโทรศัพท์ ที่ทำชื่อเสียงคือการขโมยเลขที่บัตรเครดิตและรหัสไปใช้

แฮกเกอร์เป็นบุคคลที่มีความชำนาญในด้านการใช้งานคอมพิวเตอร์ แต่นำประสบการณ์มาใช้ในทางที่ไม่ถูกต้องเท่าไร แฮกเกอร์บางครั้งก็ทำเพื่อสร้างสรรค์ แต่บางครั้งก็เป็นการทำลาย

ระบบคอมพิวเตอร์

เมื่อมองรอบตัวเราขณะใช้งานคอมพิวเตอร์ จะพบว่าบางครั้งอุปกรณ์ต่าง ๆ มีจุดบกพร่องหรือช่องทางให้ถูกโจมตีจากผู้ไม่หวังดี ในฐานะผู้ใช้เราต้องทำตัวอย่างไรจึงจะช่วยคุ้มภัยให้กับระบบของเรา

ในที่ทำงานต้องระแวดระวังไม่ให้ถูกคุกคาม เคยเห็นมาเหมือนกันครับที่เครื่องคอมพิวเตอร์จะมีสายโยงใยล็อกด้วยกุญแจกัน การเคลื่อนย้ายและเปลี่ยนแปลงอุปกรณ์ มีการเดินสายสัญญาณต่าง ๆ ผ่านท่อร้อยสาย ทำให้ยากในการเชื่อมต่อจากหน่วยงานหรือบุคคลที่ไม่พึงประสงค์

ขั้นต่อมาถ้าหากเราจะทำการลงระบบรักษาความปลอดภัยให้กับคอมพิวเตอร์ง่าย ๆ โดยการตั้งรหัสส่วนตัว หลายระดับ ให้ยากแก่การเข้าถึงระบบ

ถ้าหากยังมีการถูกจู่โจมได้อีก การติดตั้งโทรทัศน์วงจรปิดสำหรับการทำงานกับคอมพิวเตอร์ในบางครั้งอาจทำให้พนักงานตั้งใจทำงานมากยิ่งขึ้น เพราะมีคนจับตามองตลอดเวลา สำรองข้อมูลทุกวันก็เป็นอีกแนวทางหนึ่งที่จะไม่ทำให้ข้อมูลถูกทำลายหรือสูญหายได้ และให้ดียิ่งขึ้น ระบบที่ถูกพูดและกล่าวถึงมากในขณะนี้คือไฟร์วอลล์ เป็นนโยบายการป้องกันการถูกจู่โจมทั้งภายในและภายนอกของระบบคอมพิวเตอร์

การตรวจสอบหาความบกพร่องของระบบว่ามีจุดไหนทำงานไม่เป็นปกติหรือไม่ ก็เป็นการเสริมความปลอดภัยข้อมูลขึ้นอีกขั้น

แนวทางปฏิบัติสำหรับการรักษาความปลอดภัยข้อมูล

ก่อนอื่นคงจะเป็นการจัดอบรมพนักงานหรือผู้ใช้คอมพิวเตอร์ให้รู้จักการใช้คอมพิวเตอร์ให้ถูกวิธี การจัดอบรมเน้นในเรื่องความปลอดภัยและความเสียหายเมื่อข้อมูลถูกทำลาย ในหน่วยงานควรจะมีหน่วยงานที่คอยเป็นที่ปรึกษาและวางแผนในการดำเนินงานที่เกี่ยวข้องกับการใช้งานคอมพิวเตอร์และระบบเครือข่าย

มีการตรวจสอบเกี่ยวกับการใช้งานว่ามีการนำโปรแกรมมาจากที่อื่นมาใช้หรือไม่ การตรวจสอบไวรัส ตรวจสอบระบบอย่างสม่ำเสมอ ถ้าเจอไวรัสก็ให้จัดการเสีย อย่าปล่อยให้ลุกลาม เพราะข้อมูลและระบบอาจจะเกิดความเสียหายได้

สรุปได้ว่า การให้ความรู้เกี่ยวกับการทำงาน การใช้งานระบบในทางที่ถูกที่ควร ตลอดจนมีจรรยาบรรณในการใช้คอมพิวเตอร์จะเป็นส่วนที่สำคัญที่จะทำให้ระบบคอมพิวเตอร์ตลอดจนองค์กรมีความมั่นคงได้